No. 19-15472

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AMERICAN CIVIL LIBERTIES UNION FOUNDATION; AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA; ELECTRONIC FRONTIER FOUNDATION; RIANAN PFEFFERKORN,

Movants-Appellants,

v.

UNITED STATES DEPARTMENT OF JUSTICE; FACEBOOK, INC.,

Respondents-Appellees.

On Appeal from the United States District Court
for the Eastern District of California
Misc. Case No. 1:18-mc-00057-LJO-EPG

BRIEF OF AMICI CURIAE MOZILLA AND ATLASSIAN IN SUPPORT OF MOVANTS-APPELLANTS URGING REVERSAL

Marc Zwillinger
Jeffrey Landis
ZwillGen PLLC
1900 M Street, NW, Suite 250
Washington, DC 20036
(202) 296-3585

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), *amicus* Mozilla Corporation ("Mozilla") states that it is a wholly-owned subsidiary of the Mozilla Foundation, a 501(c)(3) non-profit. No publicly held corporation has an ownership stake of 10% or more in Mozilla.

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), *amicus* Atlassian Corp. ("Atlassian") states that is has no parent corporation and no publicly held corporation owns 10% or more of its stock.

/s/ Marc Zwillinger

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULES

OTHER AUTHORITIES

IDENTITY AND INTEREST OF AMICI[1]

Mozilla is a global, mission-driven organization that works with a worldwide community to create open source products like its web browser Firefox. Its mission is guided by a set of principles that recognizes, among other things, that individuals' security and privacy on the Internet are fundamental and must not be treated as optional. In furtherance of that end, Mozilla has also adopted data privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security controls and practices.

Atlassian's products help teams organize, discuss, and complete their work in a coordinated, efficient and modern fashion. Organizations use Atlassian's project tracking, content creation and sharing and real-time communication and service management products to work better together and deliver quality results on time.

INTRODUCTION

Legal decisions in United States courts are rarely maintained in complete secrecy. Cloaking legal reasoning in darkness is especially troubling where an opinion analyzes legal rights that concern matters of intense public interest. A

[1] Pursuant to Fed. R. App. P. 29(a)(2), counsel for *amici* certify that counsel for the other parties have consented to the filing of this brief. Pursuant to Fed. R. App. P. 29(A)(4)(e), counsel for *amici* state that no party's counsel authored this brief in whole or in part, and that no person other than *amici* or their counsel contributed money that was intended to fund preparing or submitting of this brief.

decision analyzing how the government may compel access to otherwise private communications is precisely such a matter. Technology companies like *amici* are profoundly interested in understanding how the law develops around enforcement actions related to other technology, platforms, and companies. This transparency enables companies to adequately interpret, and in some cases defend against, law enforcement requests and enforcement efforts. And such information is critical for enabling secure product development as well as fulsome and transparent information for end users and consumers who rely on technology companies to convey what the benefits, risks, and implications of using a product may be. Both companies and end users must be able to understand what the government can, and cannot, require providers to do.

Precedent on compelled government access is sparse. There is one on-point decision about the technical assistance provision of the Wiretap Act, and that opinion is sixteen years old and from a divided Ninth Circuit. *See In re U.S. for an Order Authorizing Roving Interception of Oral Communications*, 349 F.3d 1132 (9th Cir. 2003) ("In re Company"). How the instant Wiretap Act decision applies to current technology services that use encryption is opaque, leaving providers to speculate about the scope and source of their potential obligations to the United States government, and how that affects the design of their products and services. The only other notable decision about the scope of providers' potential assistance

obligations is a magistrate's decision under the All Writs Act in the Eastern District of New York. *See In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

The existence of sealed proceedings that, if known, could impact the interpretation of future law enforcement requests or the design of a company's products or services, raises concerns around both security and privacy. Providers must be able to understand what can be compelled—and what cannot. From that knowledge, they can develop secure products, interpret law enforcement requests, and defend against overreach should it occur. Similarly, providers cannot be assured that they can be transparent with users when rules relating to mandatory government access are hidden in secret legal opinions.

To avoid these issues, portions of the case below should be ordered unsealed, or the court below should be required to release a public summary of its legal reasoning. This remedy has been employed even in the most secretive of courts handling the most sensitive legal proceedings. *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, No. 08–01, 2008 WL 10632524, at *1 (FISA Ct. Rev. Aug. 22, 2008) ("In re Directives").[2] It should be employed here too.

---

[2] Counsel for *amici* personally argued the classified proceeding in *In re Directives*, a decision that rejected a provider's challenge to government authority under the Protect America Act, the precursor to the FISA Amendment Act. The decision of the court was released in redacted form less than five months after it was reached. That decision was released because, as the court said, "the petition presents matters

BACKGROUND

This is neither the first case where law enforcement has demanded that providers bypass encryption or otherwise redesign their systems to assist with surveillance, nor will it be the last. Here, news reports indicate that DOJ demanded that Facebook enable access to encrypted communications sent through the Facebook Messenger application as part of a criminal investigation.[3] Facebook reportedly rebuffed the DOJ's demand because Messenger allows for end-to-end encrypted communications requiring Facebook to either re-write its encryption to install a surveillance backdoor—which would threaten the platform's security for other users—or hack the government's current target. Facebook reportedly refused to do either.[4]

In opposing the DOJ's contempt motion, Facebook reportedly argued that Messenger was not covered by the statute that required providers to build their systems with wiretap capabilities (the Communications Assistance for Law

---

of both first impression and constitutional significance. At its most elemental level, the petition requires us to weigh the nation's security interests against the Fourth Amendment privacy interests of United States persons." *In re Directives*, 2008 WL 10632524, at *1. The decision here is likely of similar significance.

[3] *See* Chris Welch, *US Reportedly Pressuring Facebook to Break Messenger's Encryption Over MS-13 Investigation*, The Verge (Aug. 17, 2018), https://www.theverge.com/2018/8/17/17725368/us-government-facebook-messenger-app-encryption-ms-13.

[4] Tom McKay, *Facebook Reportedly Defeats Government Demand to Wiretap Messenger Calls*, Gizmodo (Sept. 29, 2018), https://gizmodo.com/facebook-reportedly-defeats-government-demand-to-wireta-1829416523.

Enforcement Act ("CALEA"))[5] and that re-configuring its systems would be burdensome and costly, and thus exceed the Wiretap Act's technical assistance provision.[6] *Id.* In late September 2018, news outlets reported that the district court denied the DOJ's motion in a sealed opinion—preventing the court's rationale and legal analysis from reaching the public.[7]

In November 2018, the American Civil Liberties Union Foundation, the *Washington Post*, and others asked the district court to unseal certain parts of the underlying proceedings. Importantly, they did not ask the court to unseal facts regarding the investigation, the methods law enforcement sought to use to wiretap

---

[5] Enacted in 1995, CALEA defines the circumstances in which private companies must assist law enforcement in executing authorized electronic surveillance and the nature of—and limits on—the assistance such companies must provide. *See* 47 U.S.C. § 1001 *et seq.* Notably, CALEA only requires "telecommunication carriers" to provide such assistance and excludes from that definition persons or entities providing "information services." *Id.* at §§ 1002; 1001(8). CALEA also made clear that companies do not have an obligation to assist the government with decryption of communications where the company does not retain a copy of the decryption key. *Id.* § 1002(b)(3).

[6] *See* Ellen Nakashima, *Facebook Wins Court Battle Over Law Enforcement Access to Encrypted Phone Call*, Wash. Post (Sept. 28, 2018), https://www.washingtonpost.com/world/national-security/facebook-wins-court-battle-over-law-enforcement-access-to-encrypted-phone-calls/2018/09/28/df438a6a-c33a-11e8-b338-a3289f6cb742_story.html ?utm_term=.57cfa9824a7c.

[7] *See, e.g.*, Joseph Menn & Dan Levine, *In Test Case, U.S. Fails to Force Facebook to Wiretap Messenger Calls-Sources*, Reuters (Sept. 28, 2018), https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-in-test-case-u-s-fails-to-force-facebook-to-wiretap-messenger-calls-sources-idUSKCN1M82K1 ("U.S. investigators failed in a recent courtroom effort to force Facebook to wiretap voice calls over its Messenger app in a closely watched test case.").

the targets, or technical or proprietary information about Facebook's systems. The DOJ opposed the request to unseal. ER-2 (ECF No. 26). Facebook supported the request on the condition that any disclosed materials be subject to limited redaction. *Id.* On February 11, 2019, the district court issued a five-page opinion denying the requests to unseal. This appeal followed.

ARGUMENT

I. TECHNOLOGY COMPANIES NEED ACCESS TO JUDICIAL OPINIONS THAT IMPACT THEIR USERS AND PRODUCTS

The district court's opinion and the parties' legal arguments should be partially unsealed because providers like *amici* use judicial opinions to understand their legal rights and obligations, as well as to guide internal stakeholders and end users about the nature of their products and the potential for law enforcement requests. Law enforcement regularly issues subpoenas, court orders, warrants, and Title III orders to technology providers. In 2017, the nation's top five Internet and telecommunication providers collectively received over 1,183,000 demands for user information.[8] With respect to wiretap orders specifically, the Administrative Office of United States Courts annual report to Congress ("2017 Wiretap Report")

[8] *See* 2017 transparency reports of Apple, Facebook, Google, Microsoft, Twitter, AT&T, Sprint, T-Mobile, and Verizon, available via https://www.accessnow.org/transparency-reporting-index/; and 2017 transparency report for U.S. Cellular, https://www.uscellular.com/uscellular/pdf/Transparency_Report_2017.pdf.

reported that in 2017 federal and state judges authorized 3,813 wiretaps.[9] Not a single wiretap order was reported as denied in 2017. *Id.* In some instances, such as Mozilla's, law enforcement requests are limited in frequency but still important no matter the volume. The sealed decision thus has widespread ramifications for future cases.

Notwithstanding the significant impact law enforcement requests could have on companies' systems,[10] there is little or no modern guidance on the scope of the Wiretap Act's assistance provision and only one decision under the All Writs Act. The latter came as a result of DOJ's *ex parte* application for an order compelling Apple to extract data from a locked iPhone. *See In re Apple, Inc.*, 149 F. Supp. 3d 341. After ***open briefing and public oral argument***, the court denied DOJ's application, concluding the All Writs Act could not compel Apple's assistance where Congress had enacted laws to prescribe the private sector's duties to assist law enforcement, but none of those laws imposed any obligation on Apple to provide the requested assistance. *Id.* at 355-364. The court also concluded that

---

[9] *See* Federal Judiciary, *Wiretap Report* (Last updated on Dec. 31, 2017), https://www.uscourts.gov/statistics-reports/wiretap-report-2017.

[10] The likelihood that such request could impact system design is increasing. The number of state wiretaps reported in which encryption was encountered increased from 57 in 2016 to 102 in 2017. 2017 Wiretap Report at 4. In 97 of these wiretaps, law enforcement was unable to access the text of the messages. *Id.* Similarly, 37 of the 57 federal wiretaps reported as being encrypted in 2017 could not be decrypted. *Id.*

granting the government's application would impose an undue burden on Apple. *Id.* at 373. ***The court's opinion was released publicly***, in full, with no redactions, enabling other providers to see how the court analyzed Apple's obligations.[11]

The need for publication of the opinion in this matter is even greater. The 2003 decision in *In re Company* is the sole published authority discussing the outer limits of the Wiretap Act's technical assistance provision, and parties regularly cite to it in disputes involving the limits of that provision. Consider what would have happened if *that* opinion had been sealed. The court below would have been deprived of the legal authority most relevant to the instant dispute. Keeping this case sealed would similarly deprive future courts of the only additional authority on this important issue.

Understanding when and why a redesign to facilitate government access to user data may be demanded or required is essential in allowing providers to design secure systems, communicate comprehensively about privacy and security, and possibly defend against enforcement actions. Indeed, the court in *In re Apple* recognized the importance for companies like Apple of engaging in these

[11] Indeed, the judge that issued that opinion recently authored an op-ed in the New York Times on how law enforcement surveillance is challenging our legal system, in which he noted that to the extent that judges are asked to make deliberative choices about how to balance investigative technologies against risks to personal privacy, they should "give public account of the reasoning behind their decision." *See* James Orenstein, *I'm a Judge. Here's How Surveillance is Challenging our Legal System*, New York Times (June 13, 2019), https://www.nytimes.com/2019/06/13/opinion/privacy-law-enforcment-congress.html.

behaviors, considering not just "the direct costs of compliance" for Apple, but also "the extent to which the compromise of privacy and data security that Apple promises its customers affects not only its financial bottom line, but also its decisions about the kind of corporation it aspires to be." *In re Apple*, 149 F. Supp. 3d at 369 n.34, 372.

In addition to being the right thing to do, in today's marketplace, providers must build privacy and security into their offerings or risk losing customers and face Attorney General or FTC enforcement actions.[12] Consumers are increasingly concerned about privacy and security of their information. A recent Reuters poll reports that a majority of Americans are unwilling to compromise privacy in their email, text messages, phone records, or internet activities, even to enhance national security.[13] Recent research confirms that consumers value data security—and seek

---

[12] For example, the recently enacted California Consumer Privacy Act of 2018 allows for a civil private right of action against a provider that fails to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information . . . ." *See* Cal. Civil Code § 1798.150. And in 2017, the FTC brought an enforcement action against network equipment manufacturer D-Link alleging that D-Link's promotional and marketing statements about the security of its routers were deceptive to consumers. *See* Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. D-Link Corp.*, Case No. 3:17-cv-00039 (N.D. Cal. Jan. 5 2017), https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf.

[13] Reuters & Ipsos Pub. Affairs, Cybersecurity Poll 2-3 (2017), http://fingfx.thomsonreuters.com/gfx/rngs/USA-CYBER-POLL/010040EN0YD/2017%20Reuters%20Tracking%20-%20Cybersecurity%20%20Poll%203%2031%202017.pdf.

out businesses with strong data security practices.[14] Against this backdrop, a company that does not take privacy and security seriously will not be able to compete effectively. This necessarily involves understanding what the government might successfully demand of it when designing its products and what design decisions carry legal consequences.

If something about a provider's design decision is the lynchpin in the analysis of whether a provider is covered by CALEA or otherwise can be forced to redesign its architecture for government surveillance, providers have a need and a right to know the basis for that determination. Privacy- and security-minded companies must, for example, understand—and account for in initial product design—whether any required redesign weakens overall security of their products, as well as any ancillary affects such redesign might have on their products. This is particularly important for the open source community. Among the most critical promises open source companies make to their users is that source code be available for public inspection. Security flaws in that code, or explicit intercept mechanisms built into that code, are thus also public. Those flaws can then be publicly identified and removed, and likewise users can make informed decisions

[14] PwC, Consumer Intelligence Series: Protect.me, at 3-4 (2017), https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf (noting that "85% of consumers will not do business with a company if they have concerns about its security practices" and that "71% would stop doing business with a company for giving away their sensitive data without permission").

about whether to use the product. This is critical to the value proposition and trust model for open source software. However, it requires that compiled code delivered to users be actually based upon the publicly available source code.

Moreover, if the government can make demands that undermine or circumvent a product or service's security, then it is hard to describe that system as secure—especially if such a method could weaken the security vis-à-vis non-governmental entities. If the government cannot make such a demand, providers can discuss the security of their technology with more confidence.

Finally, providers may face similar government demands and should not be forced to make legal decisions where the government has access to the legal reasoning of the decision below, and providers do not. If the court rejected DOJ's demands, providers should know why. Did the court find that as a matter of law the Wiretap Act's technical assistance provision cannot mandate a provider to redesign its system because CALEA already addresses when providers can be forced to design their systems to facilitate surveillance? Did it find that in this particular case, Facebook could not provide assistance unobtrusively and with a minimum of interference as contemplated by the Wiretap Act's technical assistance provision? Did the court find that such a redesign is allowable under law, but that in this case Facebook established it would be too costly or burdensome to accomplish? Did the court hold that Facebook Messenger is outside the scope of CALEA? The fact that

providers and the public do not know why—or even *that*—the court rejected DOJ's demands threatens the foundation of the precedential law system. *See Lowenschuss v. West Pub. Co.*, 542 F.2d 180, 185 (3d Cir. 1976) ("As ours is a common-law system based on the 'directive force' of precedents, its effective and efficient functioning demands wide dissemination of judicial decisions.") Indeed, unless a recipient company of a subsequent similar demand does a web search of past news articles, it will not even be aware that such an opinion exists, much less know that a government order was denied or what the opinion said. The existence of the case is completely absent from public case records and databases.

Denying providers access to the sealed opinion implicates their due process rights. "Due process, unlike some legal rules, is not a technical conception with a fixed content unrelated to time, place, and circumstances." *Cafeteria & Rest. Workers Union v. McElroy*, 367 U.S. 886, 895 (1961) (citation and internal quotation omitted). Rather, it "is flexible and calls for such procedural protections as the particular situation demands." *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972). In analogous situations courts have found that depriving a person of secret information can violate procedural due process. *See, e.g., Al Haramain Islamic Found., Inc. v. U.S. Dept. of Treasury*, 686 F.3d 965, 979 (9th Cir. 2012) (government use of classified information without disclosure of its contents implicates procedural due process); *Gete v. I.N.S.*, 121 F.3d 1285, 1297-98 (9th

Cir. 1997) (noting that INS failure to provide information including legal basis for vehicle seizure and statements of reasons for its denials of relief violated procedural due process). Here, the government could do exactly what due process prohibits—use aspects of the decision that may be favorable to it secure in the knowledge that providers cannot gain access to any unfavorable holdings.

II. PARTIAL UNSEALING OF THE COURT'S OPINION AND PARTIES' BRIEFS IS WARRANTED UNDER FIRST AMENDMENT AND COMMON LAW TESTS

The First Amendment requires partial unsealing of the district court's opinion and the parties' legal analyses, or the issuance of a separate legal summary. The presumed First Amendment right to access judicial records attaches when the "experience and logic" test is satisfied—that is (1) when records have historically been open to the press and general public and (2) when public access plays a significant positive role in the functioning of a particular process. *Press-Enter. Co. v. Superior Court*, 478 U.S. 1, 8 (1986). When such a right attaches it may be overcome "only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Phoenix Newspapers, Inc. v. U.S. Dist. Court for Dist. of Arizona*, 156 F.3d 940, 946 (9th Cir. 1998) (citation omitted). Here, logic and experience dictate that at least redacted versions of the court's opinion and parties' legal analyses should be released, even if wiretap application materials are traditionally sealed. Complete

sealing of the judicial decision is neither essential nor narrowly tailored to the government interest in protecting the integrity of wiretap investigations.

A. Logical Considerations Support Partial Unsealing

Logical considerations support partial unsealing of the district court's opinion and the legal analyses of the parties. Court decisions "are adjudications—direct exercises of judicial power the reasoning and substantive effect of which the public [including *amici*] has an important interest in scrutinizing." *Encyclopedia Brown Prods, Ltd. v. Home Box Office, Inc.*, 26 F. Supp. 2d 606, 612 (S.D.N.Y. 1998). Without access to such decisions, "public oversight of the courts, including the processes and the outcomes they produce, would be impossible." *Doe v. Public Citizen*, 749 F.3d 246, 267 (4th Cir. 2014). Unsealing this opinion is warranted because it is likely the first (and only) opinion regarding whether the government can use the Wiretap Act's technical assistance provision to compel an Internet provider to redesign its systems. Allowing future litigants access to the opinion for use in similar proceedings will allow for more fulsome legal argument in future law enforcement requests. It will also assist providers in developing more secure products.

Providers like *amici* must also be able to speak about the benefits, risks, and implications of using their products, and what they can and would do in response to requests from law enforcement. And they must be able to speak honestly. They

should not be forced to decide between making no representations to customers about such important issues, or making such representations at the risk of having them turn out be untrue due to unknown information. Indeed, the law prohibits such conduct. *See, e.g.*, *Zaluski v. United Am. Healthcare Corp.*, 527 F.3d 564, 572 (6th Cir. 2008) ("[O]nce a company chooses to speak, it must provide complete and non-misleading information with respect to subjects on which [it] undertakes to speak.") (citation and internal quotation omitted). Without partial unsealing, providers cannot know the extent of the demands the government might make, how courts will rule on them, and how those demands or rulings will affect their product security.

B. Experience Supports Partial Unsealing

Judicial opinions are public records. This has been the tradition for hundreds of years. Accordingly, "under our system of jurisprudence the judiciary has the duty of publishing and disseminating its decisions." *Lowenschuss*, 542 F.2d at 185; *see also In re McCormick & Company, Inc.*, Misc. No. 15-1825 (ESH), 2017 WL 2560911, at *1 (D.D.C. June 13, 2017) ("The presumption in favor of public access is especially strong for judicial orders and opinions.").

Recent experience of other courts that routinely receive highly sensitive and classified information—the Foreign Intelligence Surveillance Court ("FISC") and Foreign Intelligence Surveillance Court of Review ("FISCR")—provide a useful

model for this Court to order the release of the district court's opinion and relevant legal arguments while still protecting sensitive government information. *See El Vocero de Puerto Rico (Caribbean Int'l News Corp.) v. Puerto Rico*, 508 U.S. 147, 150 (1993) (noting that in analyzing the experience prong, courts look not only at the experience of the particular court, but also at similar types of proceedings).

Unlike the practice in traditional federal courts, since their creation in 1978 the FISC and FISCR have conducted all of their activities in secret. But even before the passage of the USA FREEDOM Act in 2015—which added a provision allowing for the public disclosure of certain opinions—these courts released important legal decisions. *See, e.g.*, *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002) (2002 decision evaluating FISC order imposing restrictions on use of information collected using the Foreign Intelligence Surveillance Act); *In re Directives*, 2008 WL 10632524 (2008 decision addressing whether directives issued to service provider to assist in warrantless surveillance of non-U.S. customers violated Fourth Amendment). And now, the USA FREEDOM Act expressly requires a declassification review of *each* decision, order or opinion the Foreign Intelligence Surveillance Court issues "that includes a significant construction or interpretation of any provision of law" and, consistent with such review, requires the government "make publicly available to the greatest extent practicable each such decision, order, or opinion." 50 U.S.C. § 1872(a). In

practice, this means that opinions stemming from matters more sensitive and secretive than this one have been released in redacted form for public access and scrutiny.[15] These releases help inform similarly-situated providers about the nature and scope of their obligations and allow them to consider such obligations when designing their products or communicating with their customers.

The FISC's handling of its 2014 *Memorandum Opinion and Order Compelling Compliance with Directives, [REDACTED], No. [REDACTED]*, GID.C.00111 (FISA Ct. 2014) (Collyer, J.) is illustrative.[16] In that case, an unnamed provider challenged compliance with directives issued to it pursuant to Section 702 of FISA. While much of the opinion is redacted—to protect both the providers information and sensitive government interests—one can nevertheless conclude from the unredacted portions of the court's order that: (1) the company's First and Fourth Amendment rights were not offended by the intelligence collection proposed in this case; (2) absent a specific flaw or failing in the government's procedures, the risk that the government might task the wrong account was not a sufficient basis to invalidate the surveillance in light of the

[15] In all, there are approximately 70 opinions and 250 orders from the FISC or FISCR publicly available in full or partially redacted form—many predating the USA FREEDOM ACT. *See* DC Digital Georgetown Foreign Intelligence Law Collection, https://repository.library.georgetown.edu/handle/10822/1052698.

[16] *Available at* http://hdl.handle.net/10822/1052720.

government's post-tasking obligations; (3) the company's interest in protecting its non-U.S. customers was inapplicable to the Court's review. *Id*. at 32-33, 36. Each of these findings helps guide future providers facing a similar demand for assistance in government surveillance.

C. The Government's Interest in Protecting the Integrity of Future Wiretap Investigations Can Be Accomplished by Redactions or a Summary of Decision

Even where the government has an interest in preserving the secrecy of law enforcement techniques in Title III wiretap cases, complete sealing of the materials requested is not narrowly tailored to meet that interest. *Amici* are not seeking release of any actual or contemplated law enforcement techniques or facts about the underlying criminal matter—only the legal analyses regarding the limits, if any, on Title III's technical assistance provision (or any other law).

The district court stated that redaction was not viable because sensitive investigatory information was so thoroughly intertwined with legal and factual arguments that redaction would leave little and/or misleading substantive information. ER-4 (ECF No. 26). But even if that were the case, whatever information is not intertwined (and does not constitute Facebook's trade secrets) should be released. The fact that the FISC and FISCR regularly release opinions that redact sensitive information but reveal legal analysis suggests the same can be accomplished with the materials here. Even so, a partially redacted opinion is but

one solution. ***This Court should also consider directing the district court to prepare a separate summary of its legal analysis that can be released.*** *See Pepsico, Inc. v. Redmond*, 46 F.3d 29 (7th Cir. 1995) (ordering district court to prepare opinion suitable for public release that referred to trade secrets indirectly, rather than keep existing opinion sealed entirely). Either way, the answer should not be that the district court's opinion on a novel legal issue that is a matter of intense public interest is kept secret from everyone but the government and parties forever.[17]

CONCLUSION

For the foregoing reasons, the Court should order the district court to release in redacted form its opinion reportedly denying the DOJ's motion for contempt against Facebook and the parties' legal analyses regarding such motion, or to create a summary of such materials suitable for public release.

RESPECTFULLY SUBMITTED,

Dated: June 19, 2019

By: */s/ Marc Zwillinger*
Marc Zwillinger
marc@zwillgen.com

[17] Partial unsealing is also warranted under common law. The Ninth Circuit recognizes "a strong presumption in favor of access to court records." *Foltz v. State Farm Mut. Auto. Ins. Co.*, 331 F.3d 1122, 1135 (9th Cir. 2003). A party seeking to seal a judicial record can only overcome this presumption by meeting the compelling reasons standard. *Id.* Here, as discussed above, while the government might have an interest in keeping its particular methods secret, these interests do not overcome the need to inform *amici* about the state of the law, especially where that interest can be accomplished via redaction.

Jeffrey Landis
jeff@zwillgen.com
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
(202) 296-3585 telephone)
(202) 706-5298 (facsimile)

Counsel for Amici

STATEMENT OF RELATED CASES

Counsel for amici states that it is aware of one related case pending in this Court, *WP Company v. United States Department of Justice*, Case No. 19-15473.

Dated: June 19, 2019 /s/ Marc Zwillinger

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 19-15472

I am the attorney or self-represented party.

This brief contains 4,605 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Marc Zwillinger **Date** June 19, 2019
(use "s/[typed name]" to sign electronically-filed documents)

CERTIFICATE OF SERVICE

I hereby certify that on June 19, 2019, the foregoing brief was served electronically via the Court's CM/ECF system upon all counsel of record.

Dated: June 19, 2019 /s/ Marc Zwillinger